



Assurance with Open Source

Anil Saldhana

Red Hat Middleware (JBoss)

Anil.Saldhana@redhat.com

<http://anil-identity.blogspot.com>

DHS SwA Forum, March 10-12, 2009

MITRE, McLean, VA

Speaker

- Lead Security Architect at Red Hat Middleware
- Red Hat representative at Security Standards at W3C, Oasis and the Java Community Process (JCP)
- Co-editor of an upcoming W3C Security Specification on Browser Security.
- Technical Lead of JBoss Common Criteria Evaluation Process.
- Open Source Champion (Bread and Butter)

Open Source Software

http://en.wikipedia.org/wiki/Open_source_software

OSS can be defined as computer software for which the human-readable source code is made available under a copyright license (or arrangement such as the public domain) that meets the Open Source Definition. This permits users to use, change, and improve the software, and to redistribute it in modified or unmodified form. It is very often developed in a public, collaborative manner.

US Federal agencies define open source as “*Commercial software whose source code available by license permitting users to study and change (improve) the software, as well as redistribute it in modified or unmodified form.*”

NOTE: Open Source Platforms from vendors have restrictive licenses as far as modification of binaries is concerned.

Assurance With Open Source Software

- Open Source delivered as a platform by a vendor such as Red Hat.
 - Red Hat Enterprise Linux (RHEL)
 - JBoss Enterprise Application Platform (EAP) etc.
- Security Assurance with the open source platform.
 - Secure Development Practices. (Proactive)
 - Security Response Team. (Proactive/Reactive)
 - Security Certification.

Assurance With Open Source Software

- Security Assurance with the open source platform.
 - Secure Development Practices. (Proactive)
 - Security Response Team. (Proactive/Reactive)
 - Security Certification.
- Tools integrated in automated builds.
- Development team has at least one mentor/supervisor who is security conscious.
 - *Preach secure development methods.*
 - *Code reviews to identify patterns of software development flaws.*
- Automated tests that grow over time to handle regressions of vulnerabilities.
 - *Ideally, every vulnerability that is fixed should have an associated test such that it does not happen again, over the life of the product.*

Assurance With Open Source Software

- Security Assurance with the open source platform.
 - Secure Development Practices. (Proactive)
 - **Security Response Team. (Proactive/Reactive)**
 - Security Certification.

- Accountable for vulnerabilities that affect RedHat products and services
 - Monitoring
 - Triage
 - Escalation and troubleshooting through life cycle
 - Communication with other affected vendors
 - Internal communication, documentation, advisory
 - Responsible for errata release
 - Metrics and feedback to Engineering

Assurance With Open Source Software

- Security Assurance with the open source platform.
 - Secure Development Practices. (Proactive)
 - Security Response Team. (Proactive/Reactive)
 - **Security Certification.**
- Common Criteria Evaluation
(<http://www.redhat.com/solutions/government/commoncriteria/>)
 - Red Hat Enterprise Linux 5
 - HP: EAL 3+/CAPP
 - IBM: EAL 4+/CAPP
 - SGI: EAL 3+/CAPP
 - UNISYS: EAL 3+/CAPP
 - JBoss Enterprise Application Platform v4.3, EAL 2 (In Evaluation)
 - Metamatrix Enterprise Data Services Platform v5.5.2, EAL 2 (In Evaluation)

Security Response Team

- Led by Mark J Cox.
- Handle 85 released Red Hat product versions. (November 2008)
- Handle, triage and investigate about 50 vulnerabilities/month.
- Staff in around 6 countries worldwide.
- In 2008, triaged 6 vulnerabilities per week.
 - *Triage involves separate issues that are important, examine the products/versions affected etc.*

Security Response - OVAL

- A machine-readable, standard way to express vulnerabilities and patch issues
 - Definitions contain details of how to test for the presence of vulnerable software
 - *can also look for vulnerable uses or configuration*
 - XML based standard
 - Modular
 - *Designed to deal with heterogeneous environments*
 - *Interoperability testing of tools and processes*



Open Vulnerability and Assessment Language

The language to determine the presence of vulnerabilities and configuration issues on computer systems

Security Response – OVAL Example

```
- <advisory from="secalert@redhat.com">
  <severity>Moderate</severity>
  <rights>Copyright 2003 Red Hat, Inc.</rights>
  <issued date="2003-11-12"/>
  <updated date="2003-11-12"/>
  <cve href="http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0925">CVE-2003-0925</cve>
  <cve href="http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0926">CVE-2003-0926</cve>
  <cve href="http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2003-0927">CVE-2003-0927</cve>
</advisory>
</metadata>
- <criteria operator="AND">
  <criterion test_ref="oval:com.redhat.rhsa:tst:20030324001" comment="Red Hat Enterprise Linux 3 is installed"/>
- <criteria operator="OR">
  - <criteria operator="AND">
    <criterion test_ref="oval:com.redhat.rhsa:tst:20030324002" comment="ethereal is earlier than 0:0.9.16-0.30E.1"/>
    <criterion test_ref="oval:com.redhat.rhsa:tst:20030324003" comment="ethereal is signed with Red Hat master key"/>
  </criteria>
  - <criteria operator="AND">
    <criterion test_ref="oval:com.redhat.rhsa:tst:20030324004" comment="ethereal-gnome is earlier than 0:0.9.16-0.30E.1"/>
    <criterion test_ref="oval:com.redhat.rhsa:tst:20030324005" comment="ethereal-gnome is signed with Red Hat master key"/>
  </criteria>
</criteria>
</criteria>
```

Security Response – Finding Vulnerability

 https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2008-1926

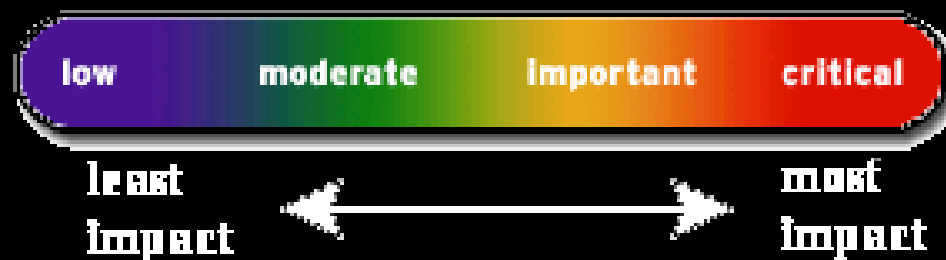
Additional Bug Information

Summary CVE-2008-1926 util-linux: audit log injection via login

URL <http://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-1926>

Status Whiteboard source=redhat,reported=20080419,public=20080421,impact=low

Keywords Security





Common Vulnerability Enumeration is a dictionary of publicly known vulnerabilities.

Security Response - CVE

The screenshot shows a web browser window with the address bar displaying <https://rhn.redhat.com/errata/CVE-2008-0072.html>. The page header includes the Red Hat Network logo and navigation links: **Errata**, **Sign In**, and **About RHN**. The main heading is **CVE-2008-0072**. The text below states: "Updated packages to correct this issue are available along with our advisory at the URLs below. Users of the Red Hat Network can update their systems using the 'up2date' tool." Under the heading "Red Hat Enterprise Linux:", two URLs are listed: <http://rhn.redhat.com/errata/RHSA-2008-0177.html> and <http://rhn.redhat.com/errata/RHSA-2008-0178.html>.

Security Response - CPE

Common Platform Enumeration is structured naming system for IT systems, platforms and packages.

```
<?xml version="1.0"?>
```

```
<cpe-list xmlns="http://cpe.mitre.org/dictionary/2.0"
```

```
  xmlns:cpe_dict="http://cpe.mitre.org/dictionary/2.0">
```

```
  <cpe-item name="cpe:/a:redhat:certificate_system:7.3">
```

```
    <title>Red Hat Certificate System 7.3 for 4AS</title>
```

```
  </cpe-item>
```

```
  <cpe-item name="cpe:/a:redhat:directory_server:8.0">
```

```
    <title>Red Hat Directory Server 8.0 (for AS v. 4)</title>
```

```
  </cpe-item>
```

```
  <cpe-item name="cpe:/a:redhat:jboss_enterprise_application_platform:4.2.0::el4">
```

```
    <title>JBoss Enterprise Application Platform for RHEL 4 AS</title>
```

```
  </cpe-item>
```

Security Response - NVD

 <https://nvd.nist.gov/nvd.cfm?cvename=CVE-2008-2420>

disclosure of information , Allows disruption of service

Vendor Statements ([disclaimer](#))

Official Statement from Red Hat (5/26/2008)

Not vulnerable. OCSP protocol support was only implemented in upstream stunnel version 4.16. Therefore OCSP protocol is not available in the versions of stunnel as shipped with Red Hat Enterprise Linux 2.1, 3, 4, or 5.

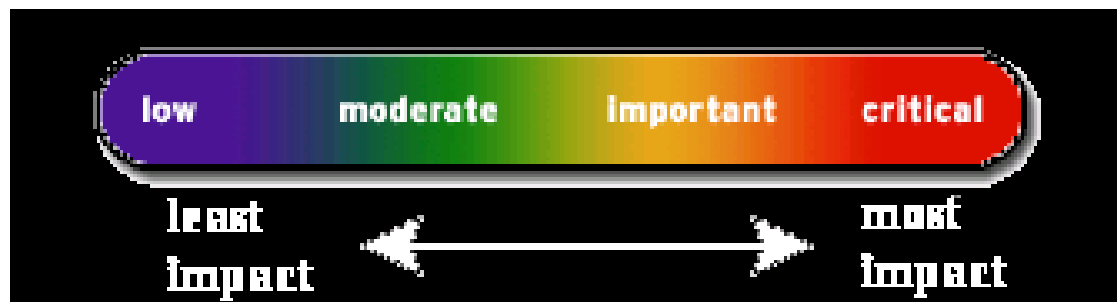
Security Response - Reporting

secalert@redhat.com

- Address used to ask vulnerabilities' related questions
 - Report new vulnerabilities
 - Ask how we addressed any particular vulnerabilities
 - Chartered to respond within 3 Business Days

Security Response – Release Policy

- Critical Vulnerabilities
 - *Pushed immediately or when embargo lifted or QE finished.*
 - *Any time of day/week – holidays/weekends.*
- Important Vulnerabilities
 - *Reasonable time and day (M-Thu)*
- Moderate or Low Vulnerabilities
 - *Next update release or wait for other issues affecting the same package.*



Security Response - Cycle

- Vulnerability reported, learned...
- Triage
- Construct the Security Errata
 - *Credit the reporters*
 - *Collate packages*
- QE
- Release
- Pick up updated packages from Red Hat Network (RHN) Channels
 - *Email alerts in RHN, enterprise-watch-list@redhat.com, rhsa-announce@redhat.com*
 - *Web : <https://rhn.redhat.com/errata/>*

Reference Links

- [RedHat] <http://www.redhat.com>
- [RedHat Security] <http://www.redhat.com/security>
- [RedHat Oval] <http://www.redhat.com/security/transparent/oval/>
- [Anil Saldhana Blog] <http://anil-identity.blogspot.com>
- [Mark J Cox Blog] <http://www.awe.com/mark/blog>



Q&A